IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Cr. No. 05-1849 JH
	)	
DANA JARVIS, et al.,	)	
	)	
Defendants.	)	

UNITED STATES' RESPONSE TO DEFENDANT OSGOOD'S "MOTION TO COMPEL DISCOVERY RELATED TO PEN REGISTER, CELL PHONE SITE, OR GPS DATA" (DOC. 1598)

The United States hereby responds to defendant George Osgood's "Motion to Compel Discovery Related to Pen Register, Cell Phone Site, or GPS Data" (Doc. 1578).

FACTUAL BACKGROUND

On March 2, 2005, DEA Special Agent Richard Stark submitted an affidavit to Senior United States District Judge John Edwards Conway in support of an application for an order authorizing the interception of wire communications of numerous listed subjects, including Dana Jarvis and David Reid, over cellular telephone number (505) 470-1811. Ultimately, between March 4 and August 25, 2005, federal agents conducted judicially authorized wiretap interceptions of eight telephones – seven cellular telephones and one landline telephone – utilized by members of the Dana Jarvis marijuana trafficking organization. In the course of the investigation in this case, prior to and during the

wiretap interceptions, agents utilized pen registers / trap and traces on certain telephones used by targets of the investigation.[1]

The initial indictment in this case was returned on August 23, 2005. On November 15, 2005, the Court entered a "Stipulated Order Setting Deadlines and Declaring Case Complex." (Doc. 258). Among other things, the order established a schedule for the production of discovery.

On July 16, 2006, the defendants who were represented by court-appointed counsel filed a "Joint Motion to Compel Discovery Related to the Interception of Electronic Communications." Doc. 573. Defendant Reid joined in the motion. Doc. 592. In that motion, the defendants requested, among other things, "all pen register records and printouts pertaining to this investigation, any of the defendants in this case, or any factual allegation made or individual referred to in the affidavits of DEA Special Agent Richard

---

[1] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n. 1 (1977). The installation and use of a pen register and trap and trace device is governed by 18 U.S.C. §§ 3121-3127. Section 3121(c) provides:

> A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(Emphasis added).

L. Stark." *Id.* at 4. In response, the United States agreed to "work with the defendants to provide them with the pen register records that they seek." Doc. 614 at 4. The Court therefore denied this request as moot. Doc. 733 at 3.

Subsequently, the United States provided the defense with a CD containing the pen register data that had been downloaded into the Penlink program by DEA in conjunction with the investigation in this case. The defendants did not request any additional information in this regard until defendants Reid, Wilson, and Hill filed their "Joint Motion to Suppress the Fruit of Title III Wiretaps" on February 2, 2009. Doc. 1533.[2] In that motion, the defendants request, *inter alia*, that the Court "order disclosure of the raw, unmanipulated data, and permit supplemental briefing if the analysis of that data indicates that post cut-through dialed digits were indeed captured before the wire intercept authorization was given." *Id.* at 62.[3]

On April 4, 2009, co-defendant George Osgood filed a motion (Doc. 1578) ("the Osgood Motion") requesting discovery related to pen registers, cell site acquisition and Global Positioning System (GPS) data. On April 20, 2009, defendant Reid filed a

---

[2] This motion was filed on February 2, 2009 pursuant to the Court's November 10, 2008 order granting in part defendant Reid's unopposed motion to extend the motions deadline. Doc. 1456.

[3] In that motion, the defendants incorrectly assert that they had previously requested this "raw data" but that the United States had "disclosed data in a manipulated format [the Penlink data] that does not permit the defense to ascertain whether content was captured or not." *Id.* at 61-62. As discussed above, the United States provided the defense with the data contained in Penlink in response to their general request for "pen register records and printouts."

pleading styled "Defendant Reid's Joinder in Defendant Osgood's Motion to Compel Discovery Related to Pen Register, Cell Phone Site, or GPS Data" (Doc. 1598). On April 23, 2009, defendant Osgood entered a plea of guilty in this case, making the motion moot as to Osgood.

With regard to defendant Reid, the Osgood Motion should be denied as untimely, as it was filed well after defendant Reid's motions deadline. But even if the Court proceeds to the merits of the motion, it should be denied for the reasons set forth below.

DISCUSSION

The Osgood Motion identifies five categories of documents that the defendant seeks: 1) Raw pen register data, cell phone site data, and GPS data on the wiretap target telephone numbers and on any phone number captured by the government in this case or a related Drug Enforcement Administration (DEA) case; 2) Applications by the government to collect such information on any telephone number of interest to the government; 3) Affidavits or other materials in support of such applications; 4) the Court orders authorizing or denying such applications; and 5) wiretap "second line data." Federal Rule of Criminal Procedure 16(a)(1)(E), provides that a defendant is entitled to:

> inspect and copy or photograph books, papers, documents, photographs, tangible objects, buildings or places, or copies or portions thereof, which are *within the possession, custody or control of the government*, and which are *material to the preparation of the defendant's defense* or are *intended for use by the government as evidence in chief at trial*, or were obtained from or belong to the defendant.

(Emphasis added). Even read generously, this rule fails to support the defendant's

requests.

1. CATEGORY 1

The items requested in Category 1 are either previously disclosed, not in existence, not material to the defense, not intended to be used by the United States in its case-in-chief, or some combination thereof.

A. "Raw" pen register data

The defendant first seeks the disclosure of the "raw pen register data" originally collected by the government. The attached affidavit of DEA Analyst Elizabeth Eller describes the procedure employed by the DEA at the time the pen registers and wiretaps in this case were executed. *See* Exhibit 1. As Analyst Eller indicates, the pen register data can be divided into two separate procedures – those related to land lines and those related to cellular service.

For cellular phones, the DEA never received any data other than through Penlink. The information was sent directly from the phone company and imported without manipulation into the Penlink software. No other equipment or machine received cellular phone pen register data. The only "raw data" was the data that is in Penlink, which has been previously produced to the defendants. Thus, at least with regard to cell phones, the defendant's request should be denied as moot.

For traditional land lines, an actual device was placed on-site for the targeted line which captured all dialed digits. The DEA, via modem, through the data collection

system, was able to access the device and download all calls captured since the prior download. The data collection system then created a file for those downloaded calls. DEA next used the Penlink software to transfer the recently created file into the Penlink system. The initial records were not analyzed, nor were they even reviewed, until they were imported into the Penlink software. This was the technology in effect at the time of the relevant pen registers.

With regard to the "raw data" that does exist, the defendant fails to show how the records he seeks are material to his defense. The only materiality reference that he makes is an oblique suggestion that this information may establish that the government did not comply with the law or that there may be exculpatory information. *See* Osgood Motion at p. 5. But materiality means more than that the evidence in question bears some abstract logical relationship to issues of the case – there must be some indication that pretrial disclosure of the disputed evidence would enable a defendant significantly to alter the quantum of proof in his favor. *See United States v. Thevis*, 84 F.R.D. 47 (N.D. Ga. 1979). And to carry his burden of making a threshold showing of materiality, *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995), "requires a presentation of 'facts which would tend to show that the Government is in possession of information helpful to the defense.'" *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)). In this regard, "[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to

show that the Government is in possession of information helpful to the defense." *Id.*

To be sure, the materiality requirement is not a heavy burden; rather, evidence is material as long as there is a strong indication that the evidence "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *Id.* at 351 (internal quotations omitted). Nevertheless, ordering the production by the government of discovery without any preliminary showing of materiality is inconsistent with Rule 16. Applying these standards to the instant case, the defendant has failed to meet his burden of demonstrating that disclosure is material to his defense and necessary for a fair trial.

The defendant does not even attempt to explain why or how the information he seeks is necessary for the preparation of his defense at trial. There is no indication that the requested documents will play any important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting in impeachment or rebuttal evidence. In fact, the defendant makes no statement at all about whether the information sought is material, claiming only that the raw data is necessary "so that he can properly analyze whether or not the government's collection of pen register data complied with the law." Osgood Motion at 4. But he cites to no statutory authority or case law that even suggests that he is in a position to do so.[4] In fact, the pen/trap statute

[4] The defendant cites to only one case in support of this request – that being the 1987 decision of *United States v. Feola*, 651 F. Supp. 1068, 1144 (S.D.N.Y. 1987). But not only does the defendant misread this 22-year old case, he assumes away the major

itself suggests that the defendant is in no position to challenge the pen register information. In contrast to the wiretap statutes at 18 U.S.C. §§ 2515, 2518(10)(a) which provides a specific exclusionary remedy, the pen register statute at 18 U.S.C. § 3121(c) provides no such remedy.

Even assuming, *arguendo*, that the pen register data in this case was collected in violation of the pen register statute, evidence obtained in violation of the statute can be admitted in criminal trials because violation of the statute does not result in an unconstitutional search and Congress did not provide for exclusion of evidence for violation of the statute. *United States v. Thompson*, 936 F.2d 1249 (11th Cir. 1991). *See also United States v. German*, 486 F.3d 849, 853-54 (5th Cir. 2007). The defendant seems to request this information as a precursor to attacking the validity of the wiretap evidence in this case. *Thompson* squarely shuts down the defendant's inquiry even if he were able to prove that the pen registers in this case were illegally obtained.

---

technology differences that exist today. First, the defendant's reading of *Feola* ignores that the discovery order in relation to the pen register tapes was apparently in the context of the government's use of such information as evidence at trial, not a challenge to a wiretap order. Here, the government is not using the pen register information obtained independent of the wiretap orders themselves at trial. Second, in relying on *Feola*, the defendant assumes that there are, in fact, "pen register tapes." Clearly technology has advanced since the district court in *Feola* had cause to review the technology surrounding pen registers. As Analyst Eller's affidavit makes clear, the pen register information is no longer contained on a "tape." Rather the pen register process is automated to the point that all information is directly imported into Penlink – software which can read this computerized information. As discussed above, the government has previously produced the data from Penlink to the defendants.

In *Thompson*, the defendant filed a motion to suppress information gained from an illegally obtained pen register. There was no disagreement that the information from the pen register was, in fact, illegally obtained. The defendant claimed that since such information was utilized to support probable cause in an affidavit supporting a Title III wiretap, the information obtained through the wiretap must also be excluded. In rejecting the defendant's claim, the court found no constitutional or statutory basis to support the defendant's claim, and specifically held, "that information obtained from a pen register placed on a telephone can be used as evidence in a criminal trial even if the court order authorizing its installation does not comply with the statutory requirements." *Thompson*, 936 F.2d at 1249-1250.

Here, there is nothing to suggest that any of the pen register information was illegally obtained. But more importantly, even if any of the information was illegally obtained the wiretap evidence in this case would be unaffected. Therefore, the defendant's request for this data should be denied.[5]

B. Cell Phone Site Data

Cell site information is non-content information maintained by wireless carriers. It is useful to law enforcement for the limited information it provides about the location of a cell phone when a call was made. "The information does not provide a 'virtual map' of

[5] The United States also objects to the defendant's request for data relating to "any phone number captured by the government in this case or a related DEA case that may have been used in this case," Osgood Motion at 2, as being over-broad.

the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower." *In re Application of United States for an Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005).

Defendant offers no support to suggest that cell site information is discoverable at this time. The government has not indicated that any of this information will be utilized at trial. And the defendant has not suggested how any of this information is material to his defense. Until such time that the government indicates that such evidence will be used a trial, the defendant has no authority under Rule 16 or elsewhere mandating the disclosure of such information.

C. GPS Data

No GPS data was requested or collected in relation to any telephone number in this investigation. Therefore, this request should be denied as moot.

2. CATEGORY 2 – Applications by the Government for Pen Registers, Cell Site, or GPS Data

With respect to any applications made by the government for pen register, cell site information or GPS information, the defendant again cites no authority which requires disclosure of such information. In his attempt to acquire this information the defendant hoists himself as the gatekeeper for whether the government has "complied with the Federal Rule of Criminal Procedure 41." However, Rule 41 is not implicated by any of the information received by the government. The collection of pen register information is

governed by 18 U.S.C. § 3122. And as the United States Supreme Court has acknowledged, a person enjoys no expectation of privacy in the dialed digits of their telephone and the retrieval of such information does not amount to a search under the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735 (1979). Again, unlike the wiretap statute which specifically requires disclosure of the applications for a wiretap, there is no statutory requirement that the application for a pen register be disclosed. Similarly, the acquisition of cell site information is governed by 18 U.S.C. § 2703 and not Rule 41. The defendant again points to no authority that even suggests that applications by an attorney for the government are subject to disclosure under Rule 16. Furthermore, to the extent that the defendant's requests covers "any number of interest to the government," Osgood Motion at 3, it is entirely too broad.

3. CATEGORY 3 – Affidavits Submitted in Support of Applications by the Government for Pen Registers, Cell Site, or GPS Data

Defendant requests affidavits and or other materials filed in support of applications for pen register or cell site information. There are no affidavits or other accompanying materials in support of any of the applications for pen register or cell site information. Accordingly, this request is moot and should be denied.

4. CATEGORY 4 – Court Orders Authorizing or Denying Pen Registers, Cell Site, or GPS Data

Defendant seeks any and all court orders that authorized the government to collect the pen register and cell site data in this case. Again, as with his request for applications

made by the government, the defendant fails to demonstrate any support that these orders are discoverable.

5. CATEGORY 5: "Wiretap Second Line Data"

Defendant requests information related to "second line data" which includes text messaging. Defendant makes this request on information and belief as to the mechanics involved in the interception of wire communications. There was, however, no text messaging or other electronic information intercepted in this case.

CONCLUSION

Fed. R. Crim. P. 16 does not entitle the defendant to "wide –ranging discovery to canvass for evidence in support of [a] motion to suppress." *United States v. Harding*, 273 F. Supp. 2d 411, 430 (S.D.N.Y. 2003). The defendant may not use Rule 16 as a fishing expedition. *United States v. Marazino*, 860 F.2d 981, 985-86 (10th Cir. 1988). To allow speculative irrelevant discovery would do just that. The defendant's claims that the requested information is necessary as a precursor to a challenge to the wiretap evidence is contradicted by the pen register statute itself which does not require the exclusion of evidence obtained in violation of its provisions. In sum, the defendant has completely failed to make the particularized showing that is necessary for the pre-trial disclosure of the requested material. Accordingly, the defendant's motion should be denied in its entirety.

Respectfully submitted,

GREGORY J. FOURATT
United States Attorney

/s/ James R.W. Braun

JAMES R.W. BRAUN
Assistant U.S. Attorney
P.O. Box 607
Albuquerque, NM 87103
(505) 346-7274

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 11th day of May, 2009, I filed the foregoing pleading electronically through the CM/ECF system, which is designed to cause counsel of record for the defendants to be served by electronic means.

ELECTRONICALLY FILED

JAMES R.W. BRAUN
Assistant U.S. Attorney